Project Closure Report

Authorization Interoperability

(A project under the umbrella of the VO Services Project)

Table of Contents

Approvals

OSG Customer and Sponsor	**Signature:**	
	Print Name:	Mine Altunay
	Title:	
	Date:	
Project Manager:	**Signature:**	(approved)
	Print Name:	Gabriele Garzoglio
	Title:	Application Developer and System Analyst
	Date:	Jun 16, 2009

Document Change Log

Revision	Date	Change Description	Prepared By	Approved By
v0.1	11/18/08	Initial text	Gabriele Garzoglio	
v0.2	12/04/08	Text mature enough for initial internal review	Gabriele Garzoglio	
v0.3	03/19/09	Updating the text with latest developments	Gabriele Garzoglio	
v1.0	04/03/09	Finalizing the document	Gabriele Garzoglio	
v1.1/2	06/16/09	Adding post-deployment comments	Gabriele Garzoglio	

Project Abstract

Goal of the Authorization Interoperability activity is providing interoperability between middleware and authorization infrastructures. This is achieved by agreeing on and implementing an authorization protocol common to OSG VO services, EGEE, Globus, and Condor.

This protocol is used by Policy Enforcement Points (PEP), i.e. resource gateways, to interact with Policy Decision Points (PDP), i.e. repository of authorization policies. For each access request, the PDP informs the PEP on whether access is granted or denied and, what obligations need to be enforced if access if granted. Obligations are used as a mechanism to restrict privileges at Grid resources.

Project Documentation

This section provides links to project definition documents and initial plan.

Exploratory Meeting of OSG VO Services and Globus (10/2006)
http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=239

Meeting: OSG VO Services and Globus define the collaboration (2/2007)
http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=323

Meeting: EGEE comes on board (4/2007)
http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=333

Project web page:
http://www.fnal.gov/docs/products/voprivilege/focus/AuthZInterop/info.html

- Minutes and material from all collaboration meetings (about 70 meetings)
- Software and documentation deliverables
- Presentations and intermediate documentation.

Supporting Documentation

This section lists the documentation developed during the definition and execution of the project. The following link provides context and support for closing the project.

Authorization Interoperability Profile:
FNAL doc db (2952) and CERN EDMS (929867)
This document defines the common authorization interoperability protocol and profile and is a major deliverable of the project.

Software libraries used to implement the specifications in the Authorization Interoperability Profile:

- Java: OpenSAML2.0 Extension Library to Support SAML2.0 Profile of XACML2.0: http://opensaml.org
  For this deliverable, our collaboration has worked with Internet 2 through the EGEE / SWITCH group.
- C: Globus Toolkit implementation of the SAML 2.0 Profile of XACML v2.0: http://www-unix.mcs.anl.gov/~bester/xacml/

Deployment document: “The Deployment of Authorization Interoperability-enabled Middleware on OSG and EGEE”
http://www.fnal.gov/docs/products/voprivilege/focus/AuthZInterop/documents/AuthZ%20Interop%20Deployment%20v0.5.doc

Reason for Closing the Project

The project has achieved its main goals, throughout the 1.5 years of the project. A discussion of the difference between planned and achieved deliverables is available in the “Project Deliverables” section.

Project Deliverables

This section lists high-level deliverables for the projects.

Planned Deliverables	**Actual Deliverables**
An XACML Attribute	An XACML Attribute and Obligation Profile for Authorization

and Obligation Profile for Authorization Interoperability in Grids	Interoperability for the uses cases of OSG, EGEE, Globus, and Condor. This document defines the specification of the common authorization protocol.
Libraries implementing the SAML v2 profile of XACML v2	Java implementation through Internet2 OpenSAML and C implementation through the Globus Toolkit.
Common libraries implementing the Authorization Interoperability Profile	This code is a very thin layer on top of the SAML v2 / XACML v2 libraries. Common libraries make sense only for middleware with established maintenance agreement. Common libraries have been implemented for - gPlazma and GUMS (privilege.jar); this is reused by other Java implementations, such as BeStMan. - SCAS client/server and PRIMA / gLExec: these are C implementations; the PRIMA module reuses most of the SCAS client libraries for its implementation. The Globus Toolkit has implemented the profile for the GT security framework.
Integration of the Authorization Interoperability protocol with all relevant middleware and policy decision points used by OSG and EGEE	The Authorization Interoperability protocol has been integrated with the following middleware (see table 1 for a summary): - GT pre-WS Gatekeeper (a.k.a. GT2 gatekeeper): integrated in OSG through the PRIMA call-out module; in EGEE through the SCAS client module. VO Services maintenance of the new interface is less than of the old interface because some common libraries are maintained by Globus and EGEE. - GT GridFTP: integrated in OSG through the PRIMA module, in EGEE through the SCAS client module. Native support is being developed as of Mar 2009. - gLExec: integrated through the EGEE LCAS/LCMAPS (L&L) authorization framework. In EGEE, L&L invokes a SCAS client module. In OSG, L&L calls a wrapper to the PRIMA module. The same wrapper also invokes a gLExec monitoring process; if monitoring could be factorized out, then gLExec could be configured to call-out through the SCAS client module, instead of PRIMA, like EGEE does. This would reduce further the VO Service maintenance load. - GT4.2 WS-GRAM: integrated through a native call-out interface. This interface supports only the Username obligation (OSG use case). Support for the obligations necessary to integrate with the EGEE framework has been discussed and considered low priority (see bugzilla bug #6109). - SRM / dCache: integrated through the gPlazma call-out module. This module shares libraries (such as privilege.jar) with the GUMS server interface. - CREAM: integrated in EGEE through gLExec. The Authorization Interoperability protocol has been integrated

with the following Policy Decision Points (PDP):

- GUMS: this is the PDP used in OSG. GUMS supports the interoperability interface as well as the legacy SAML v1 interface, used until the OSG v1.0 release.
- SCAS: this is the PDP used in EGEE. SCAS supports only the interoperability interface.
- We did early tests (Oct 2007) of the interoperability protocol with XACML engine PDPs, such as gJAF and GPBox, used by some EGEE deployments. Because these PDPs are not widely deployed, full integration tests have not been completed.

Middleware	AuthZ Call-out Module		Resource Controlled
	OSG	EGEE	
pre-WS Gatekeeper	PRIMA	SCAS	CE
WS Gatekeeper	Native	N/A	CE
CREAM	N/A	gLExec	CE
SRM/dCache	gPlazma	gPlazma	SE
GridFTP	PRIMA	SCAS	SE
gLExec	Native	Native	WN

Table 1: The following table summarizes the middleware integrated with the Authorization Interoperability protocol and the call-out modules used in each case.

Integration of the following middleware has not been achieved by this project; however it is desirable, with different degrees of priority:

- GT 4.2 RFT and Delegation services: in cooperation with the WS-GRAM service (see above), these services allow for managing complex remote jobs. This work is required to use the GT4.2 services for the job management use cases of OSG users. The GT team defined a plan for this work: see http://bugzilla.mcs.anl.gov/globus/ bug keyword “OSG/EGEE_Authz_Interop”. The plan will be executed when OSG commits to deploy the GT4.2 services. This integration has medium priority.
- GT v4.2 WS-GRAM does NOT support EGEE obligations (UIDGID, etc.). EGEE does not plan to deploy GT v4.2 in the near future, so this limitation is accepted by the collaboration.
- GT GridFTP native support: the current support is through the PRIMA module. Development of this feature is under way, as of Jun 2009: see bugzilla bug #6526. The Globus priority for this work seems very low. This integration has medium priority.
- GT pre-WS Gatekeeper native support: the current support is

	through the PRIMA module. There is no plan to implement this feature. This integration has low priority. - GT 4.0 WS-GRAM native support: the current support is through the PRIMA-WS module. This module supports only the legacy call-out protocol, based on SAML v1. Support for this service may dictate when support for the legacy protocol can be discontinued. Support for GT4.0 should be discontinued after GT4.2 is deployed on OSG. There is no plan to implement this feature. This integration has low priority. - gJAF and GPBox: these are authorization systems developed in the context of EGEE. The systems are based on pure XACML engines as PDPs. The projects have been heavily involved in the definition of the interoperability profile. It was demonstrated in a test environment that the systems could use authorization policies derived from the profile. The systems were never used in production with these policies, though. Authorization projects, after the closing of this one, should work with EGEE to understand the role of these technologies. This work as a low priotity. - Condor and Condor-G: integration is possible as per the common profile, but the development work has not been scheduled. The authorization call-out could be used to map user grid credentials to the condor canonical user i.e. the owner of a condor job. Currently, Condor uses other mechanisms, such as gridmap-files, for authorization. This integration has low priority. Integration of the following PDP has not been achieved by this project, even if it is desirable: - Site Authorization Service (SAZ): the SAZ team was involved in the definition of the Authorization Interoperability profile. Because of internal priorities and personnel issues, the SAZ project could not follow up with the development of the new interface until Mar 2009. The development is in progress, but considered out of the scope of the Authorization Interoperability project. In addition, the implementation of the following call-out modules have these limitations: - PRIMA - It does not implement validation of the VOMS attribute certificates. This limits the reusability of PRIMA as a generic call-out module. - It does not implement the handling of pilot attributes from the environment context. - It cannot distinguish between the action attributes "execute-now" and "queue", when formatting authorization request, because the globus gatekeeper does not pass job-manager information to the call-out module. This is an issue with the GT pre-WS

	authorization call-out interface. - "Optional attributes" from the profile are not implemented - Prima implements no-op obligation handlers for the afs-token and secondary-gids obligations. All other unknown obligations deny access. This is compliant with the XACML specification. - SCAS client: - It does not implement the handling of pilot attributes from the environment context - It cannot distinguish between the action attributes "execute-now" and "queue", as for PRIMA. - These optional subject attributes are not implemented: cert-chain, ca-policy-oid, and ca-serial-number - It does not implement obligation handlers for all obligations. The ones that are not known throw an exception, therefore deny access authorization: this is compliant with the XACML specifications. - The implementation of c libraries can be optimized to improve performance further. We watched the CPU and load of the server machine as the number of clients increased. We observed a sub-linear growth of resource consumption vs. number of clients, an indication that the library can be improved to handle authorization requests more efficiently. The inefficiency is either in SCAS code (Oscar Koeroo), in the C XACML implementation (Joe Bester), or in the gSOAP libraries. - gPlazma: - The glite trustmanager v1.8.16-1 implementation of the AxisSocketFactory was found to have a memory leak. The leak was fixed by Ted Hesselroth for dCache use and a description of the problem and new code was transmitted through the GGUS ticketing system and to the developer via email. - It does not implement optional subject attributes in the XACML request and does not support VOMS-signing-issuer. - It does not implement obligation handlers for all obligations. It throws an exception for unknown obligations, as SCAS does. - GT 4.2 Security framework: - It does not implement the handling of pilot attributes from the environment context - It does not implement support for the following optional subject attributes: certificate-serial-number, cert-chain, ca-policy-oid, and ca-serial-number - It implements support for the username obligation only. - It does not deny authorization for unknown obligation. This is a problem of compliance with the XACML

	specification and GT has opened a bug for it: http://bugzilla.mcs.anl.gov/globus/show_bug.cgi?id=6568

Change Requests	**Impact**
The development team charged with implementing the SAML2 / XACML2 specification changed from Globus Toolkit to EGEE/SWITCH	At the MWSG 13, in Dec 2007, the collaboration decided to stop the efforts of the Globus Toolkit to develop the SAML2 / XACML2 specification and to adopt the implementation of the OpenSAML group, sponsored by Internet2 and developed in collaboration with the EGEE/SWITCH group. The transition was beneficial to stop duplication of work. It resulted in about a month of delay on the initial schedule to bring the SWITCH group on board and to understand the new library.
A common attribute parser for extended VOMS proxies.	Common libraries for parsing proxies represented an opportunity to reduce maintenance of authorization modules. For java implementations, the development of a common library was framed as a Globus Incubator Project. FNAL, ANL, and INFN-Bologna formed a collaboration to work on the project, called "VOMS Policy Information Point (PIP)". This required the development of a Software Collaboration Agreement between FNAL and ANL. Such agreement can be now reused for similar joint projects. For C implementations, the integration of a common library has not been attempted, as each system had parsing capabilities already. Because of personnel personal issues, the project is currently (Mar 09) in hold. This effort is deemed lower priority than other deliverables.

Project Schedule

This section discusses the schedule of major milestones (or "Project Phases" as per the table below).

Project Phases	**Planned Completion Date**	**Actual Completion Date**
Project concepts exploration: Exploration of initial concepts between the OSG VO Services project and the Globus Toolkit (GT).	-	Oct 2006
Project definition: The OSG VO Service project and GT agree on a program of work of common interest: the development of a modern interoperability authorization call-out interface.	Early 2007	Feb 2007
EGEE joins the collaboration: EGEE had planned to evolve their authorization system (LCAS/LCMAPS) from offering local authorization only to a site-central authorization service on the internet (SCAS). They planned to focus effort on it in Aug 2007.	-	Apr 2007
GT releases alpha implementation of XACML2 specs: Globus releases the alpha version of the java and C libraries that implemented the specification. Both libraries	Aug 2007	Aug 2007

were used for early real-life tests of different formulations of the authorization interoperability specifications. The java implementation was later on abandoned in favor of the OpenSAML library (see below). GT kept the responsibility for developing the C library of the specification.		
Change of the SAML2/XACML2 development team: To avoid duplication of work, the collaboration decided to adopt the OpenSAML implementation of the SAML2/XACML2 specification. Discussion started in Sep 2007 and converged in Dec 2007 with the decision to switch development team. The collaboration developed a plan for the transition.	Dec 2007	Jan 2008
GT releases 1st stable library for XACML2 in C: GT releases a usable implementation of the SAML2 / XACML2 specification in C. Initial tests in Jan showed that improvements are needed. The library has been actively maintained after the initial release.	Jan 2008	Jan 2008
Condor joins the collaboration: Condor participates to the definition of a common authorization interoperability protocol for use cases related to condor.	Mid 2007	Feb 2008
Release of 1st stable library of OpenSAML (Java): The EGEE / SWITCH development team releases the java library for the XACML2 specification.	Feb 28, 2008	Mar 3, 2008
Release of the Authorization Interoperability profile: This document defines the specification of the attributes relevant to authorization requests and responses. Until Oct 2007, the collaboration focused on the “obligation” and “subject” attributes; in Nov 2007, it became clear that the document had also to detail the other elements of the XACML model for authorization (“resource”, “action”, and “environment” attributes). Once understood the extended scope, it was clear that the initial deadline needed to be revised. The extended timeline gave Condor the opportunity to join the group.	Dec 2007	May 2008
Completed the Integration and interoperability tests of the new protocol with middleware: During the first half of 2008, collaborating groups have integrated their middleware with the new protocol (see “Project Deliverables”). Plans for the interoperability tests between C and Java libraries started in Jan 2008. As developers integrated the authorization interoperability protocol with the each piece of middleware, we tested authorization against SCAS and GUMS servers. This continuous testing phases, started in late Jul 2008, uncovered problems in the various implementations, until all major problems were fixed in early Oct 2008.	Aug 2008	Oct 2008
Packaging of the new middleware: VDT committed to packaging PRIMA, gLExec, GUMS,	Oct 2008	Dec 2008

and dCache. The packaging was delayed because of some internal delayes of VDT and some last minute problem with the software.		
Certification of the new middleware for production: EGEE certification process is ongoing. SCAS client and gLExec has passed certification in March. SCAS server certification is delayed, because operations are challenged by a memory leak in the C XAML library. Globus is currently investigating mitigations to this problem. OSG ITB tests will certify the AuthZ software stack for production by the end of Mar. dCache v1.9.2-4 / gPlazma implements the new XACML protocol, but will be certified by ITB in the next testing cycle (possibly in Apr 09).	Nov 2008	Mar 2009
Verification that production deployments are robust: OSG v1.0.1 has run the infrastructure in production for about 2 months with no trouble tickets. EGEE runs gLExec and SCAS in production at Nikhef and several Pre-Production Sites are involved.	May 2009	Jun 2009

Project Team

The team was composed by members of 9 institutions in the EU and the US. The team had 18 active members (listed below) and 25 participants overall. In the table below, members from FNAL are shaded in grey.

Name	**Project Role**	**Ramp-down Plan**	**Timeframe**
Gabriele Garzoglio	Project Coordinator (FNAL)	Move to a liaison role after project is closed	Early 2009
Igor Sfiligoi	VO Services developer for PRIMA and gLExec (FNAL)	Move to maintenance of PRIMA and gLExec after testing and deployment	Early 2009
Jay Packard	VO Services developer for GUMS (BNL)	Move to maintenance of new interface for GUMS after testing and deployment	Early 2009
Ted Hesselroth	dCache developer for gPlazma (FNAL)	Move to maintenance of gPlazma after testing and deployment are done	Early 2009
Valery Sergeev	SAZ developer (FNAL)	No longer on the project	-
Neha Sharma	SAZ developer (FNAL)	Move to maintenance of the new interface for SAZ, after development, testing, and deployment are done.	Early 2009
Rachana Ananthakrishnan	GT 4.2 developer / Java expert	Outside of the control of the Project Coordinator. Expected maintenance	-

	(ANL)	responsibilities for GT4.2 services.	
Joe Bester	GT developer / C expert	Outside of the control of the Project Coordinator. Expected maintenance responsibilities for XACML2 implementation in C.	-
Frank Siebenlist	GT expert in security and XACML (ANL)	Consultation only	-
Oscar Koeroo	EGEE Security developer for EGEE authorization services (Nikhef)	Outside of the control of the Project Coordinator. Expected maintenance responsibilities for SCAS libraries and gLExec.	-
Yuri Demchenko	EGEE expert in security and XACML; gJAF developer (U. of Amsterdam)	No longer on the project	-
Chad La Joie	OpenSAML Project Manager (SWITCH)	Already on a maintenance role for OpenSAML	-
Håkon Sagehaug	OpenSAML developer (BCCS)	No longer on the project	-
Andrea Ferraro	GPBox developer (INFN-Bologna)	No longer on the project	-
Alberto Forti	GPBox developer (INFN-Bologna)	No longer on the project	-
Vincenzo Ciaschini	EGEE expert in security (INGN-Bologna)	No longer on the project	-
Ian Alderman	Condor developer (U. of Wisconsin)	No longer on the project	-
Zach Miller	Condor developer (U. of Wisconsin)	No longer on the project	-

Budget and Financial Information

M&S budget did not require additions to the regular development platforms for the VO Services project and for other middleware project (dCache and SAZ)

S&W budget:

- Effort was limited to a few FTE hours per month from Oct 2006 to May 2007. The effort consisted in attending meetings and thinking about authorization interoperability, as the collaboration was being formed and work defined.
- Effort picked up between June 2007 and Aug 2008, but at FNAL remained within the levels allocated for the VO Services project (0.8 FTE) and other middleware projects.
- Effort peaked between Sep and Mar 2008, in an effort to close out the project. In particular, Coordination and gPlazma development work tended to go above budgeted limits for an overall 50% FTE month.

Financial advantages of the project

- Reduced maintenance for the components maintained by the VO Services and other middleware projects. Maintenance for PRIMA, parts of gLExec, gPLazma, and SAZ was responsibility of FNAL teams. The new protocol allows for reusing common libraries developed by Globus and EGEE, thus delegating some of the responsibility for maintenance. We envision that in 12 months, we could start a project to integrate the OSG middleware with the gLite LCAS / LCMAPS framework, thus reducing maintenance of VO Services components even further (see “Next Step” and fig 1). This is possible because EGEE and OSG now share a common protocol.
- PRIMA-WS implements the legacy authorization protocol for the Web Service (WS) suite of GT services v4.0. By collaborating with the Globus Toolkit team, we envision a full integration of the GT v4.2 WS services with the common authorization interoperability protocol (see “Project Deliverables”). The GT v4.2 software suite can replace the GT4.0 services in OSG deployments. Despite the low level of maintenance required, we plan to withdraw support for the PRIMA-WS module in 12 months.
- The Globus Toolkit is implementing a native call-out XACML module (as of Mar 09). This will substitute PRIMA in future releases of the OSG software stack.
- The old PRIMA code was based on unmaintained libraries (SAML v1). Despite the code being stable, this entailed the risk of the need to employ large amount of effort to investigate potential regular or security bugs. We plan to phase out that code in 12 months.
- The collaboration between ANL and FNAL required investigating collaborative agreements for software development, as part of the VOMS PIP Globus Incubator Project (see “Project Deliverables”). Such agreement can be reused for future ANL / FNAL collaborations.
- The collaboration has fostered the communication between members of EGEE and of OSG on matters of Grid security and technology. The facilitated communication has largely benefited our regular development and operational activities.

Outstanding Risks

The following section describes risks with the software produced by this project.

- The software developed relies on libraries developed by the collaborating groups. We have experience with some of them (e.g. EGEE / Nikhef for gLExec, or GT for pre-WS software) on the level of support provided for their software. We do not have experience with other groups (e.g. EGEE / SWITCH for OpenSAML). In addition, this is new software, probably not free from defects. As this is new software and new groups, a risk is that the support is not to the expected level. Our mitigation strategy is maintaining initiallly periodic communication with the relevant group leaders to impress the importance of this software for OSG and EGEE operations.

- GT 4.2 has integrated the new protocol with the WS-GRAM service. This represents a proof-of-principle. In order for GT4.2 to be used to handle complex jobs, though, other services, such as Delegation and Reliable File Transfer, must be integrated as well. This project has reviewed the plans generated by GT for such integration. GT, however, will not schedule the work until OSG schedules a timeframe for the packaging of GT4.2 in the OSG software stack. On the other hand, OSG might be tempted to delay the integration of GT4.2 until fully integrated. This vicious circle represents a risk for the deployment of the authorization interoperability software. In addition, the VO Services project has decided not to integrate the new protocol with PRIMA-WS, the call-out module for GT4.0, with the idea to withdraw support for the module as GT4.2 gets deployed. Therefore, a delay in the GT4.2 deployment represents a delay in our ability to reduce maintenance for the VO Services modules. As a mitigation strategy, the project is rallying support from interested OSG parties for the packaging of GT4.2 in the OSG stack.
- The authorization interoperability protocol is based on commonly agreed specification for an authorization profile (see “Project Deliverables”). Since the document was officially released, the group has discussed possible new use cases, resulting in modification to the profile. A risk is that different groups extend the specification to introduce new use cases, without seeking agreement on the changes with the rest of the collaboration. Maintaining good communication with the group members of the collaboration is our mitigation strategy. This is becoming more pressing now that the new EGEE Authorization Service is being certified for production: the service adopts a profile that is similar but not 100% compliant with the agree one.

Operations and Support

The Authorization Interoperability project was a collaboration that involved several providers of middleware. Operations, maintenance, and support for each component rest with the individual provider. The sections below describe operations, support, and maintenance for the common software.

Operations

The authorization interoperability project provides libraries to enable a new communication protocol for authorization call-outs. These libraries are never operated by themselves, but always as part of a piece of middleware. Operations of each piece of middleware rest with the middleware provider.

Maintenance and support

Maintenance responsibilities are assigned as follows:

1. **OpenSAML Java implementation of the SAML 2 / XACML 2 profile**. This library provides a Java API to format authorization assertions in the SAML 2 profile of XACML 2. All authorization modules developed in Java depend on this library. It was developed and will be maintained by EGEE / SWITCH, among others, for Internet2. Our contact for maintenance is Chad La Joie (chad.lajoie@switch.ch), the project manager of OpenSAML. The user mailing list is mace-opensaml-

users@internet2.edu. Support can be solicited through the mailing list. Typically, we expect middleware developers to request support for this library.

2. **Globus Toolkit C implementation of the SAML 2 / XACML 2 profile**. This library offers the same functionalities for the C language as OpenSAML for Java. All authorization modules developed in C depend on this library. It was developed and will be maintained by the Globus Toolkit. The main developer is Joe Bester (bester@mcs.anl.gov). Our contacts for the Security work in GT were Rachana Ananthakrishnan (ranantha@mcs.anl.gov) and Frank Siebenlist (franks@mcs.anl.gov). Support for this library should be solicited via our contacts. Typically, we expect middleware developers to request support for this library.
3. **Java implementation of the Authorization Interoperability profile (privilege.jar)**. This java library, called privilege.jar, offers facilities to implement SAML 2 / XACML 2 message communication based on the Authorization Interoperability profile. This library depends on OpenSAML and it is integrated with gPlazma and GUMS. BeStMan is a piece of middleware that will potentially also integrate privilege.jar. It was developed by Ted Hesselroth (tdh@fnal.gov), with contributions by Jay Packard (jpackard@bnl.gov), and maintained by Ted Hesselroth. Support can be solicited via our contacts, by sending an email to the privilege_project@fnal.gov mailing list, or by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org). Typically, we expect middleware developers to request support for this library.
4. **SCAS libraries**. This C library offers similar functionality to privilege.jar. This library depends on the Globus Toolkit C implementation of the SAML 2 / XACML 2 profile and it is integrated with PRIMA and gLExec.. It was developed and is maintained by Nikhef. The main developer and contact person is Oscar Koeroo (okoeroo@nikhef.nl). Support can be solicited via Oscar Koeroo, or via the mailing list grid-mw-security@nikhef.nl, or by opening a Global Grid User Support (GGUS) ticket (https://gus.fzk.de/pages/ticket.php). Since we use these libraries as part of other modules, we expect that mainly developers will request support for these components.
5. **PRIMA**: This module implements the authorization call-out for middleware developed in C. It depends on the SCAS libraries and it is used by the GT pre-WS gatekeeper, gridftp, and gLExec. It was developed and maintained by the VO Services project. Igor Sfiligoi (sfiligoi@fnal.gov) is the main contact. Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org).
6. **gLExec**. This executable command implements a POSIX UID-switching tool. It depends on PRIMA and the LCAS/LCMAPS framework (maintained by Oscar Koeroo, Nikhef). It is used by job management systems, such as GlideIn WMS and Panda. It is developed and maintained by Nikhef. The main developer and contact person is Oscar Koeroo (okoeroo@nikhef.nl). Support for developers can be obtained via Oscar Koeroo, via the mailing list grid-mw-security@nikhef.nl, or by opening a GGUS ticket (https://gus.fzk.de/pages/ticket.php). Support for OSG is provided by the VO Services project and will transition to the GlideIn WMS project. The OSG contact person is Igor Sfiligoi (sfiligoi@fnal.gov). Support for OSG users can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org).
7. **gPazma**. This module implements the authorization call-out for SRM/dCache. It depends of privilege.jar. It is developed and maintained by the dCache project. The contact developer is Ted Hesselroth (tdh@fnal.gov). Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org) or through the dCache support channels.

8. **GUMS**. This server implements a Policy Decision Point and is deployed in OSG as a user mapping service. It depends on privilege.jar. It is developed and maintained by BNL, under the umbrella of the VO Service project. The contact developer is Jay Packard (jpackard@bnl.gov). Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org).
9. **SAZ.** This server implements a Policy Decision Point and is deployed at FermiGrid as an authorization service. This service is currently being integrated with the authorization interoperability libraries. It will depend on privilege.jar. It is developed and maintained by the FermiGrid project. The project manager is Keith Chadwick (Chadwick@fnal.gov) and the main developer is Neha Sharma (neha@fnal.gov). Support can be solicited by opening a Fermilab Helpdesk ticket (helpdesk@fnal.gov) or by contacting the project manager.
10. **SCAS server**. This server implements a Policy Decision Point and is deployed in EGEE as a mapping and authorization service. It depends on the SCAS libraries. It is developed and maintained by Nikhef. The main developer and contact person is Oscar Koeroo (okoeroo@nikhef.nl). Support can be solicited by opening a Global Grid User Support ticket (https://gus.fzk.de/pages/ticket.php).
11. **Globus Toolkit 4.2 services.** This is suite of grid middleware services. The security framework in this GT release supports the authorization interoperability protocol and depends on OpenSAML. The Delegation and Reliable File Transfer (RFT) services do not currently support the interoperability protocol, although development plans have been written. Our contacts for the Security work in GT are Rachana Ananthakrishnan (ranantha@mcs.anl.gov) and Frank Siebenlist (franks@mcs.anl.gov). Support can be solicited through a series of mailing lists; bug can be submitted through the Bugzilla tracking system; details at http://www.globus.org/toolkit/support.html

Next Steps

These are proposed future work in the context of the closing project

- Follow up with the development of a native XACML call-out module for GridFTP.
- Follow up with integration of the new protocol with the GT4.2 services (see “Project Deliverable” and “Outstanding Risks”). This entails following up with the VDT team to package GT4.2 in the OSG software stack.
- Provide consultation time for the integration of the protocol with other OSG middleware. For example, BeStMan has worked on the integration of the software in May 2009 and is planning to work more on it In Aug 2009.
- Work with the collaborators to define a new forum / project for future authorization interoperability work. In particular, follow up with EGEE on the new gLite infrastructure for authorization and policy.
- The OGSA-Authorization Working Group (OGSA-AuthZ WG) of the Open Grid Forum (OGF) has been working for the past few years on a profile that would include the profile delivered by this group. When this project started, the OGSA-AuthZ WG profile did not address use cases relevant to our collaboration and was not actively developed. Instead of incurring in the overhead of a large OGF WG, we decided to develop a subset of the OGSA-AuthZ WG profile. In doing so, we strived to maintain consistency with the overall direction of the WG, by enlisting three members of the WG as our collaborators. The efforts of the WG have recently actively resumed
- Fig 1 shows a diagram of the dependencies of the middleware integrated with the Authorization Interoperability components. The diagram shows the dependencies as

of now (Mar 2009) and as foreseen for Jan 2010. Because we share a common protocol for authorization call-outs, we can now share also implementations and drastically reduce the maintenance burden of our community. The diagram shows that in one year, it is foreseeable retiring the VO Services authorization call-out components, in favor of the EGEE LCAS / LCMAPS framework configured to use a SCAS client plug in ("L&L" light-yellow boxes). This step cannot be taken immediately, because of three main reasons:

1. We want to support the legacy SAML v1 protocol for at least one year, before requiring that every site upgrades to the latest version of GUMS.
2. Not all functionalities are cleanly separated between components. For example, gLExec uses a wrapper around PRIMA for authorization call-out; the same wrapper, though, also launches a process monitor, used by the Gratia and GlideIn WMS systems for job accounting. Before gLExec can abandon the PRIMA wrapper in favor of LCAL / LCMAPS, the gLExec development team, in collaboration with Gratia and GlideIn WMS projects, must implement a different invocation method for the process monitor.
3. The SAZ project might want a gradual transition from the current SAZ-specific client (see "Internal" SAZ interface), to an XACML v2-compliant client, to no client at all i.e. using the LCAS / LCAMAPS framework with a SCAS client plug-in.

The diagram also shows the intention to drop support for the GT v4.0 Web Services Gatekeeper ("WS GK v4.0"). We believe that it is foreseeable abandoning this gateway in favor or the GT v4.2 Web Services Gatekeeper. The latter natively interfaces to the WLCG authorization frameworks via the GT Security infrastructure. Negotiations to package GT v4.2 in VDT are under way.

Lessons Learned

The following are the lessons learned from working on the project

- Early in the project, the group has taken the strategic decision to develop a profile that was a subset of a larger Open Grid Forum (OSG) Working Group deliverable, the OGSA-AuthZ profile. Our concern was that working within the constraints of a large OGF collaboration could slow the process to a halt. In addition, at the time, the WG was not active. We learned that it was very important having members of the OGSA-AuthZ WG in our collaboration, to avoid diverging from the direction of the larger AuthZ scope. In addition, we could take advantage of some of the experience gained by the WG. Now that our deliverable is done, we have a good hope to be able to plug our contribution in the larger AuthZ scope.
- One of the major delays of our project was due to underestimating the scope of the profile document. When working on such specification, we learned that it is not always easy grasping the overall picture when devising a working schedule. Seeking frequent feedback from the experts on the scope of such documents may mitigate divergence from the schedule.
- Investigations of features and scope of software projects under development may be deceiving. Our collaboration investigated whether the OpenSAML libraries could be used by our software, at a time when OpenSAML was still in the development phase. Our conclusion was that OpenSAML was not suitable. Therefore, the Globus Toolkit started the development of the same specifications (SAML v2 / XACML v2) as implemented by OpenSAML, thus duplicating effort. Despite the fact that in Dec 2007 we decided to adopt the OpenSAML libraries, this was still the impression of our collaboration on OpenSAML in Sep 2007:

1) OpenSAML v1 is not developed anymore; support has been dropped
2) today, OpenSAML v2 only provides an alpha implementation
3) there are no published milestones defined by the OpenSAML v2 development group
4) Java bindings in OpenSAML v2 still need a lot of work. For example, we cannot depend on them in their current form for the GT releases.
5) Globus is committed to working to address the requirements of our collaboration, with the right priority.

We speculate that this problem could have been caused by uncertainties in the OpenSAML leadership on the ability to deliver a working library within the constraints of our schedule. An identified problem was the lack of a publicly available OpenSAML project schedule.

- The project WBS planned for the release of a single prototype release of each middleware call-out module. This breakdown structure did not capture the fluid nature of our development, whereby several incrementally scoped prototypes were presented, until the production version was ready. This approach is natural in development activities and is best captured by extreme programming methodologies, rather than by the waterfall method, typical of our project management culture. In addition, the distributed nature of our collaborations makes it difficult to follow a waterfall model, as there is little control over resources geographically distributed. We propose the more active integration of extreme programming methodologies in our project management practices.
- Our collaboration consisted of independent software groups, such as the Globus Toolkit, EGEE/Nikhef, the OSG VO Services project, etc. Each group had the responsibility of integrating the new protocol with their middleware. The project WBS was built around common major deliverables, such as “Integrate beta release of libraries with middleware”, “integrate final release of libraries with middleware”, “test middleware interoperability”, etc. Under each deliverable, the WBS listed the activity of each software group, e.g. “Integrate GT with common libraries”, “Integrate VO Services software with common libraries”, etc. (note that these items are for exemplification purposes only). Because each software group was independent and had different schedule constraints, the schedule was difficult to follow and represent e.g. via Gnatt charts. A better organization of the WBS would have grouped deliverables for each software group.

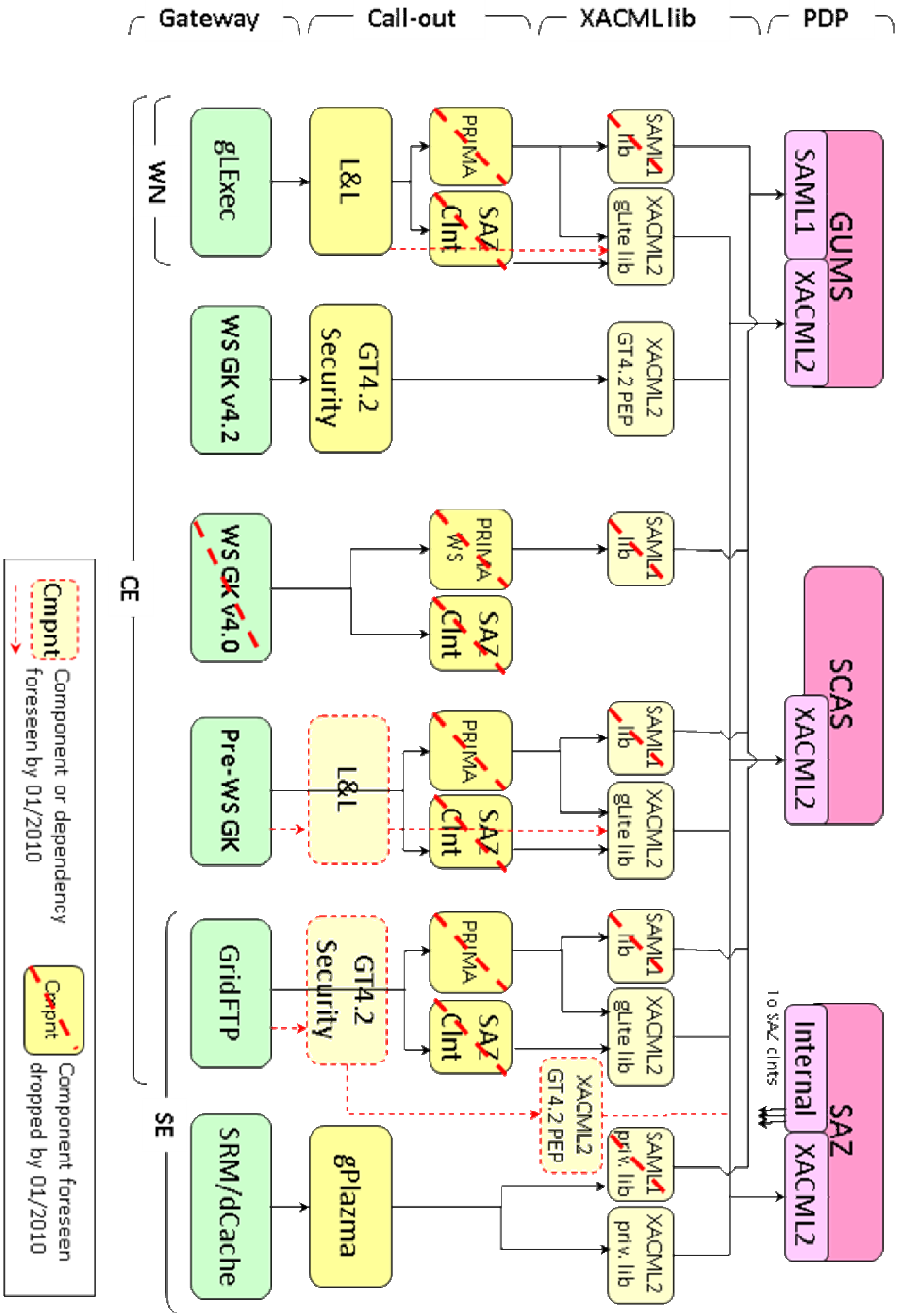

Fig. 1: Deployment of the components early on 2009 and foreseen early on 2010.